



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/652,010	08/29/2003	Art H. Burget	200207300-1	9679
22879 7590 03/06/2008 HEWLETT PACKARD COMPANY P O BOX 272400, 3404 E. HARMONY ROAD INTELLECTUAL PROPERTY ADMINISTRATION FORT COLLINS, CO 80527-2400				
EXAMINER MOORTHY, ARAVIND K				
ART UNIT 2131		PAPER NUMBER		
NOTIFICATION DATE 03/06/2008		DELIVERY MODE ELECTRONIC		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM

mkraft@hp.com

ipa.mail@hp.com

# Office Action Summary

**Application No.**

10/652,010

**Applicant(s)**

BURGET ET AL.

**Examiner**

Aravind K. Moorthy

**Art Unit**

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 17 January 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-46 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-46 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 August 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/5508)
- Paper No(s)/Mail Date see attachment
- 4) ☐ Interview Summary (PTO-413)
- Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. This is in response to the communications filed on 17 January 2007.
2. Claims 1-46 are pending in the application.
3. Claims 1-46 have been rejected.

#### ***Information Disclosure Statement***

4. The examiner has considered the information disclosure statement (IDS) filed on 29 August 2003.

#### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

**5. Claims 1-46 are rejected under 35 U.S.C. 102(e) as being anticipated by Slick et al U.S. Patent No. 7,305,556 B2.**

As to claim 1, Slick et al discloses a method of controlling use of a printer on a network, the method comprising providing a key to a client on the network [column 6, lines 37-49], wherein the key is used to submit a print job from the client to a printer on the network [column 6, lines 37-49].

As to claim 2, Slick et al discloses using the key to encrypt the print job on the client prior to transmission of the print job to the printer [column 6, lines 37-49].

As to claim 3, Slick et al discloses using the key or a related key to decrypt the print job for use by the printer [column 10, lines 16-37].

As to claim 4, Slick et al discloses that the key is specific to a particular user, the method further comprising using the key to submit the print job from the client device only at the request of the particular user [column 9, lines 25-29].

As to claim 5, Slick et al discloses generating [column 6, lines 50-62] the key with a print server [column 6, lines 14-17] on the network.

As to claims 6 and 15, Slick et al discloses the method further comprising:

storing a related key on a storage device of the print server [column 8, lines 9-17];

associating the key with a printer driver for the printer [column 8, lines 9-17]; and

installing the driver and associated key on the client [column 8, lines 9-17].

As to claims 7, 16, 21 and 33, Slick et al discloses the method further comprising:

encrypting the print job with the key resulting in an encrypted print job [column 6, lines 37-49];

sending the encrypted print job from the client to the print server [column 6, lines 37-49]; and

attempting to decrypt the encrypted print job with the related key stored on the storage device of the print server [column 11, lines 36-53];

wherein, if the related key correctly matches the key used to generate the encrypted print job, the print server successfully decrypts the encrypted print job and causes the printer to print the print job [column 11, lines 36-53].

As to claim 8, Slick et al discloses that installing the driver further comprises re-installing the driver with the associated key on the client if a driver without the key is already installed on the client [column 6, lines 22-36].

As to claim 9, Slick et al discloses that installing the driver further comprises re-configuring the driver on the client with the associated key if a driver without the key is already installed on the client [column 11, lines 16-35].

As to claim 10, Slick et al discloses that installing the driver with the associated key further comprises installing the key on the client without installing the driver if a driver configured to use the key is already installed on the client [column 6, lines 22-36].

As to claims 11, 17, 23 and 35, Slick et al discloses that the key allows the client to print to multiple networked printers managed by the print server [column 6, lines 8-21].

As to claims 12, 18, 24 and 36, Slick et al discloses that the key is provided to multiple clients [column 6 line 50 to column 7 line 4].

As to claim 13, Slick et al discloses a method of controlling a user's ability to cause a client to send a print job to a printer [column 6, lines 37-49]. Slick et al discloses the method comprising providing the client with a key specifically configured for the user [column 6, lines 37-49], wherein the client will refuse to submit a print job to the printer for a particular user unless the key associated with that user has been provided to the client [column 12, lines 1-23].

As to claim 14, Slick et al discloses the method further comprising:

generating the key with a print server [column 6 line 50 to column 7 line 4]; and

transmitting the key to the client from the print server over a network to which the print server, client and printer are all connected [column 6 line 50 to column 7 line 4].

As to claim 19, Slick et al discloses a system for controlling a client's ability to send a print job to a printer on a network, the system comprising:

at least one client [column 10, lines 59-61];

a print server for managing distribution of print jobs to one or more printers [column 9, lines 18-47]; and

a network connecting the at least one client device, the print server and the one or more printers [column 9, lines 18-47];

wherein the print server requires a client to use a key provided to the client when the client is submitting a print job to the print server [column 9, lines 18-47].

As to claim 20, Slick et al discloses that the print server is configured to:

generate the key with a utility [column 6 line 50 to column 7 line 4];

store a related key on a storage device [column 6 line 50 to column 7 line 4];

associate the key with a printer driver for the printer [column 6 line 50 to column 7 line 4]; and

install the key in association with the printer driver on the client [column 6 line 50 to column 7 line 4].

As to claim 22, Slick et al discloses that if the related key correctly matches the key used to generate the encrypted print job, the print server successfully decrypts the encrypted print job and causes the printer to print the print job [column 12, lines 1-23].

As to claim 25, Slick et al discloses that the key allows any user to cause the client to send the print job to the print server [column 9, lines 18-47].

As to claim 26, Slick et al discloses that the at least one client comprises a personal computer [column 5, lines 35-45].

As to claims 27 and 37, Slick et al discloses that the configuration utility is an embedded web server that resides on the print server [column 9, lines 18-47].

As to claim 28, Slick et al discloses that the storage device is incorporated into the print server [column 9, lines 18-47].

As to claim 29, Slick et al discloses that the storage device is connected to the network, but separate from the print server [column 9, lines 18-47].

As to claim 30, Slick et al discloses a system for controlling a user's ability to cause a client to print a print job to a printer on a network, the system comprising:

a client [column 9, lines 18-47]; and

a print server for managing at least one network printer, wherein the print server provides a key to the client for use in submitting a print job, the key being specific to a particular user of the client [column 9, lines 18-47];

wherein the client will refuse to submit a print job for a user unless the client has been previously provided with a key specific to that user [column 12, lines 1-23].

As to claim 31, Slick et al discloses that the print server comprises:

a configuration utility for configuring the key [column 7, lines 44-61]; and  
a storage device for storing a related key [column 7, lines 44-61].

As to claim 32, Slick et al discloses that the print server:

configures the key specifically for the user with the configuration utility [column 7, lines 44-61];

stores a related key on the storage device [column 7, lines 44-61];

associates the key with a printer driver for the printer [column 7, lines 44-61]; and

installs the key in association with the driver on the client [column 7, lines 44-61].



As to claim 34, Slick et al discloses that if the related key correctly matches the key used to generate the encrypted print job, the print server successfully decrypts the encrypted print job and causes the printer to print the print job [column 11, lines 36-53].

As to claim 38, Slick et al discloses a system controlling use of a printer on a network, the system comprising:

a client connected to the network for generating a print job for the printer [column 9, lines 18-47]; and

means for providing a key to the client, wherein the key is used to submit a print job from the client to the printer [column 9, lines 18-47].

As to claim 39, Slick et al discloses means on the client for encrypting the print job using the key to produce an encrypted print job for transmission to the printer [column 10, lines 16-37].

As to claim 40, Slick et al discloses decryption means for using a related key to decrypt the print job for use by the printer [column 11, lines 36-53].

As to claim 41, Slick et al discloses that the decryption means comprise a printer server [column 11, lines 36-53].

As to claim 42, Slick et al discloses that the key is used by multiple clients on the network [column 6, lines 8-21].

As to claim 43, Slick et al discloses that the key is specific to a particular user, the client being configured to use the key to submit the print job only at the request of the particular user [column 7, lines 44-61].

As to claim 44, Slick et al discloses that the means for providing a key comprise a print server on the network [column 6, lines 8-21].

As to claim 45, Slick et al discloses that the printer server further comprises:

means for storing a related key on a storage device of the print server  
[column 9, lines 18-47];

means for associating the key with a printer driver for the printer [column  
9, lines 18-47]; and

means for installing the key in association with the printer driver on the  
client [column 9, lines 18-47].

As to claim 46, Slick et al discloses that the printer server further comprises:

means for attempting to decrypt the encrypted print job with a related key  
[column 11, lines 36-53];

wherein, if the related key correctly matches the key used to  
generate the encrypted print job, the print server successfully decrypts the  
encrypted print job and causes the printer to print the print job [column 11,  
lines 36-53].

***Conclusion***

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/  
Examiner, Art Unit 2131

/Ayaz R. Sheikh/  
Supervisory Patent Examiner, Art Unit 2131